CS-459

Foundations of probabilistic proofs

Chiesa Alessandro

Cursus	Sem.	Type
Computer science	MA1, MA3	Opt.
Cyber security minor	H	Opt.
Cybersecurity	MA1, MA3	Opt.
Ing.-math	MA1, MA3	Opt.
Mathématicien	MA1, MA3	Opt.
SC master EPFL	MA1, MA3	Opt.

Language of teaching	English
Credits	6
Session	Winter
Semester	Fall
Exam	During the semester
Workload	180h
Weeks	14
Hours	**5 weekly**
Lecture	4 weekly
Exercises	1 weekly
Number of positions	

Summary

Probabilistic proof systems (eg PCPs and IPs) have had a tremendous impact on theoretical computer science, as well as on real-world secure systems. They underlie delegation of computation protocols and hardness of approximation. This course covers the foundations of probabilistic proof systems.

Content

Proofs are at the foundations of mathematics, and verifying the correctness of a mathematical proof is a fundamental computational task. (The P versus NP problem, which deals precisely with the complexity of proof verification, is one of the most important open problems in all of mathematics.) The complexity-theoretic study of proof verification has led to new notions of mathematical proofs, such as Interactive Proofs, Probabilistically Checkable Proofs, and others.
Probabilistic proofs are a powerful tool for proving hardness of approximation results, and are an essential building block to achieve delegation of computation (protocols that enable super fast verification of long computations, such as SNARKs). Via these applications, probabilistic proofs have had a tremendous impact on theoretical computer science and, more recently, are playing an exciting role in applied cryptography, computer security, and blockchain technology (e.g., they help secure billions of dollars in transactionds per day).
This course provides an introduction to probabilistic proofs and the beautiful mathematics underlying them.
Covered topics include arithmetization, the sumcheck protocol, zero knowledge, doubly-efficient interactive proofs, linearity testing, low-degree testing, proof composition, succinct verification, and more.
This courses assumes basic familiarity with algorithms (asymptotic notation and analysis of algorithms), complexity theory (computation models and simple complexity classes), and some algebra (finite fields and their properties).

Learning Prerequisites

Recommended courses

- CS-250 Algorithms
- CS-251 Theory of Computation

Important concepts to start the course

- Basic knowledge of discrete probability.
- Basic knowledge of finite fields and their properties.
- Basic knowledge of algorithms (asymptotic notation and analysis of algorithms).
- Basic knowledge of computational complexity (Turing machines; boolean circuits; complexity classes; reductions, familiarity with the classes P and NP; probabilistic computation and the class BPP).

Learning Outcomes

By the end of the course, the student must be able to:

- Understand different models of probabilistic proofs
- Analyze the security of probabilistic proofs protocols and how general computations are probabilistically checked

Teaching methods

Two weekly lectures that include definitions, theorems, and proofs. One weekly recitation to guide students through exercises. Weekly problem sets to reinforce the material.

Expected student activities

- Attend lectures and participate in class
- Complete homework assignments
- Complete a final exam or final project

Assessment methods

- Class participation (5%)
- Homeworks (55%)
- Exam or project (40%)

Supervision

Office hours	Yes
Assistants	Yes
Forum	Yes

Resources

Moodle Link

- https://go.epfl.ch/CS-459